

日 本 国 特 許 庁
JAPAN PATENT OFFICE

10.12.03

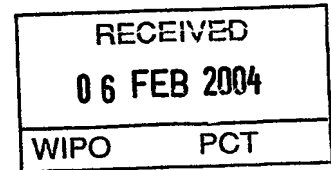
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2002年12月11日

出 願 番 号
Application Number: 特願2002-359597
[ST. 10/C]: [JP2002-359597]

出 願 人
Applicant(s): インターレックス株式会社

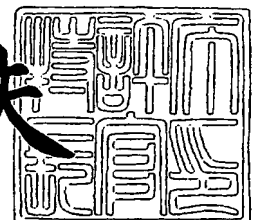


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 1月22日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 PI020121
【あて先】 特許庁長官殿
【国際特許分類】 G06F 1/00

【発明者】

【住所又は居所】 東京都港区芝浦 2 - 1 7 - 1 3 インターレックス株式
会社内

【氏名】 佐藤 健次

【特許出願人】

【識別番号】 500058589

【氏名又は名称】 インターレックス株式会社

【代理人】

【識別番号】 100095371

【弁理士】

【氏名又は名称】 上村 輝之

【選任した代理人】

【識別番号】 100089277

【弁理士】

【氏名又は名称】 宮川 長夫

【選任した代理人】

【識別番号】 100104891

【弁理士】

【氏名又は名称】 中村 猛

【手数料の表示】

【予納台帳番号】 043557

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1



【物件名】

要約書 1

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 ソフトウェア更新システム及びソフトウェアの実行制御プログラム

【特許請求の範囲】

【請求項1】 ユーザコンピュータにインストールされた第1のソフトウェアを第2のソフトウェアに更新させるソフトウェア更新システムであって、

エンコードされた前記第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行制御プログラムを前記ユーザコンピュータに通信ネットワークを介して配信する配信手段と、

前記ユーザコンピュータにインストールされた前記実行制御プログラムからの要求によってユーザ認証を行い、正当なユーザであると確認した場合には、前記第2のソフトウェアをデコードして起動させるために必要な所定の情報を前記通信ネットワークを介して前記実行制御プログラムに送信する認証手段と、を備え、

前記第2のソフトウェアは前記実行制御プログラムから渡される起動情報のみで起動可能に構成されており、

前記実行制御プログラムは、

- (1) 前記認証手段から受信した前記所定の情報に基づいて前記エンコードされた第2のソフトウェアをデコードして前記第1のソフトウェアに置き換え、
- (2) 前記所定の情報に基づいて起動情報を生成することにより、前記第2のソフトウェアを起動させ、
- (3) 前記第2のソフトウェアの実行が終了された場合には、前記第2のソフトウェアを無力化させるように構成されているソフトウェア更新システム。

【請求項2】

前記実行制御プログラムは、複数種類の第2のソフトウェアに対応可能に構成されており、

前記認証手段が前記実行制御プログラムに送信する前記所定の情報には、起動させる第2のソフトウェアの格納先アドレス情報と起動引数と第2のソフトウェアをデコードするためのデコードキー情報とが含まれている請求項1に記載のソ

ソフトウェア更新システム。

【請求項 3】

前記実行制御プログラムは、前記ユーザコンピュータに固有のマシン情報と暗号化キー情報とを含む認証用情報を前記認証手段に送信し、

前記認証手段は、少なくとも前記マシン情報に基づいてユーザ認証を行い、正当なユーザであると確認した場合には、前記所定の情報を前記暗号化キー情報で暗号化して前記通信ネットワークを介して前記実行制御プログラムに送信するものであり、

かつ、前記認証手段には、前記マシン情報を複数個登録可能である請求項 1 に記載のソフトウェア更新システム。

【請求項 4】

前記認証手段は、正当なユーザであると確認した場合には、該ユーザが起動可能な第 2 のソフトウェアの一覧データを前記ユーザコンピュータに送信し、前記一覧データから選択された第 2 のソフトウェアに関する前記所定の情報を前記通信ネットワークを介して前記実行制御プログラムに送信するものである請求項 1 に記載のソフトウェア更新システム。

【請求項 5】

前記実行制御プログラムは、

前記ユーザコンピュータに固有のマシン情報を取得する機能と、

暗号化キー情報を生成する機能と、

前記認証手段にユーザ認証を要求し、少なくとも前記マシン情報及び前記暗号化キー情報を前記認証手段に送信する機能と、

前記認証手段から受信した起動可能な第 2 のソフトウェアの一覧データからいずれか 1 つの第 2 のソフトウェアをユーザに選択させ、選択された第 2 のソフトウェアを前記認証手段に通知する機能と、

前記選択された第 2 のソフトウェアの前記ユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを少なくとも前記暗号化キー情報により暗号化してなる所定の情報を受信する機能と、

前記暗号化された所定の情報を少なくとも前記暗号化キー情報により解読する

機能と、

前記解読されたデコードキー情報により前記ユーザコンピュータ内の第2のソフトウェアをデコードさせる機能と、

前記解読された起動引数及び前記格納先アドレス情報に基づいて、前記起動情報を生成する機能と、

前記生成された起動情報によって前記デコードされた第2のソフトウェアを起動させる機能と、

前記起動された第2のソフトウェアの実行状態を監視し、該第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアを無力化させる機能と、を前記ユーザコンピュータ上に実現させるものである請求項1に記載のソフトウェア更新システム。

【請求項6】

前記第2のソフトウェアは、プログラムと付随データ群とを含んでなり、前記プログラム又は前記付随データ群の少なくともいずれか一方を更新させるものである請求項1に記載のソフトウェア更新システム。

【請求項7】

前記ユーザコンピュータにインストールされている前記第1のソフトウェアは、前記第2のソフトウェアに置換されるまでは、前記認証手段による認証を受けることなく実行可能である請求項1に記載のソフトウェア更新システム。

【請求項8】

前記実行制御プログラムは、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアの全部又は一部を削除することにより無力化させるものである請求項1に記載のソフトウェア更新システム。

【請求項9】

前記第2のソフトウェアは、プログラムと付随データ群とを含んでなり、前記実行制御プログラムは、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアのエンコードデータは保存しつつ、前記デコードされた第2のソフトウェアのうち前記プログラムのみを無力化させるものである請求項1に記載のソフトウェア更新システム。

【請求項 10】

前記実行制御プログラムは、前記第2のソフトウェアとは別に強制終了させることができないプログラムとして構成されている請求項1に記載のソフトウェア更新システム。

【請求項 11】

前記配信手段と前記認証手段とは、それぞれ別体のコンピュータ上に実現されている請求項1に記載のソフトウェア更新システム。

【請求項 12】 ユーザコンピュータにインストールされた第1のソフトウェアを第2のソフトウェアに更新し、この第2のソフトウェアの実行を制御する実行制御プログラムであって、

外部の認証手段と通信ネットワークを介して通信し、ユーザ認証を求める第1の機能と、

前記認証手段から受信した所定の情報に基づいて、前記第2のソフトウェアを起動させるための起動情報を生成する第2の機能と、

前記認証手段から受信した所定の情報に基づいて、前記第2のソフトウェアをデコードさせる第3の機能と、

前記ユーザコンピュータに既にインストールされている更新前のソフトウェアを前記デコードされた第2のソフトウェアに置き換える第4の機能と、

前記生成された起動情報によって前記第2のソフトウェアを起動させる第5の機能と、

前記第2のソフトウェアの実行状態を監視し、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアを無力化させる第6の機能と、

を前記ユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

【請求項 13】

前記第2のソフトウェアは、プログラムと付随データ群とを含んでなり、

前記第4の機能は、前記プログラム又は前記付随データ群の少なくともいずれか一方を置き換えるものである請求項12に記載のソフトウェアの実行制御プログラム。

【請求項 14】

前記ユーザコンピュータに既にインストールされている更新前のソフトウェアは、前記第4の機能によって前記第2のソフトウェアに置換される前は、前記認証手段による認証を受けることなく実行可能である請求項13に記載のソフトウェアの実行制御プログラム。

【請求項15】

前記第6の機能は、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアの全部又は一部を削除することにより無力化させるものである請求項14に記載のソフトウェアの実行制御プログラム。

【請求項16】

前記第2のソフトウェアは、プログラムと付随データ群とを含んでなり、
前記第6の機能は、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアのエンコードデータは保存しつつ、前記デコードされた第2のソフトウェアのうち前記プログラムのみを無力化させるものである請求項14に記載のソフトウェアの実行制御プログラム。

【請求項17】

前記実行制御プログラムは、前記第2のソフトウェアとは別に強制終了させることができないプログラムとして構成されている請求項12に記載のソフトウェアの実行制御プログラム。

【請求項18】 ユーザコンピュータにインストールされたソフトウェアを第2のソフトウェアに更新し、この第2のソフトウェアの実行を制御する実行制御プログラムであって、

前記ユーザコンピュータに固有のマシン情報を取得する機能と、

暗号化キー情報を生成する機能と、

外部の認証手段にユーザ認証を要求し、少なくとも前記マシン情報及び前記暗号化キー情報を前記認証手段に送信する機能と、

前記認証手段から受信した起動可能な第2のソフトウェアの一覧データからいずれか1つの第2のソフトウェアをユーザに選択させ、選択された第2のソフトウェアを前記認証手段に通知する機能と、

前記選択された第2のソフトウェアの前記ユーザコンピュータにおける格納先

アドレス情報と起動引数とデコードキー情報とを前記暗号化キー情報により暗号化してなる所定の情報を受信する機能と、

前記暗号化された所定の情報を少なくとも前記暗号化キー情報により解読する機能と、

前記解読されたデコードキー情報により前記ユーザコンピュータ内の第2のソフトウェアをデコードさせる機能と、

前記解読された起動引数及び前記格納先アドレス情報に基づいて、前記起動情報を生成する機能と、

前記生成された起動情報によって前記デコードされた第2のソフトウェアを起動させる機能と、

前記起動された第2のソフトウェアの実行状態を監視し、該第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアを無力化させる機能と、
を前記ユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

【請求項19】

ユーザコンピュータにインストールされている自由に使用可能な第1のソフトウェアを第2のソフトウェアに更新可能である旨をユーザに通知させるステップと、

前記第2のソフトウェアを配信する配信用コンピュータに前記ユーザコンピュータを通信ネットワークを介して接続させ、前記第2のソフトウェアへの更新を要求させるステップと、

前記配信用コンピュータから前記ユーザコンピュータにエンコードされた前記第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行制御プログラムを通信ネットワークを介して送信させるステップと、

前記ユーザコンピュータ上で起動した前記実行制御プログラムにより、前記ユーザコンピュータと認証用コンピュータとを通信ネットワークを介して接続させ、前記認証用コンピュータにユーザ認証を要求させるステップと、

前記ユーザ認証により正当なユーザであると認められた場合に前記認証用コンピュータから前記ユーザコンピュータに送信される所定の情報に基づいて、前記第2のソフトウェアをデコードするステップと、

前記認証用コンピュータから受信した前記所定の情報に基づいて、前記第2のソフトウェアを起動させるための起動情報を生成させるステップと、

前記生成された起動情報によって前記第2のソフトウェアを起動させるステップと、

前記起動された第2のソフトウェアの実行を監視し、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアを無力化させるステップと、を含んでなるソフトウェアの更新方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば、ゲームソフトウェア、文書や図形等を作成する実務用ソフトウェア等の各種アプリケーションソフトウェアを新バージョンのソフトウェアに更新させ、その実行を制御するソフトウェア更新システム及びソフトウェアの実行制御プログラムに関する。

【0002】

【従来の技術】

一般的に、例えば、パーソナルコンピュータや携帯情報端末等のユーザコンピュータ上で稼働するゲームソフトウェア等のアプリケーションソフトウェアは、例えば、OS (Operating System)、使用言語、ハードウェア構成等の各種のソフトウェア実行環境に応じて、あるいは、ソフトウェアの価格や代金支払いの有無等に応じて、複数種類のバージョンが用意されることがある。

【0003】

例えば、同じソフトウェアであっても、英語版、日本語版、中国語版等のように、使用言語毎に異なるバージョンが用意されることがある。また、無償で提供するバージョンと有償で提供するバージョンとを用意し、無償のソフトウェアから有償のソフトウェアへバージョンアップを誘導することも比較的よく行われている。無償のソフトウェアは、「体験版」や「お試し版」とも呼ばれ、有償のソフトウェアは「製品版」や「完全版」とも呼ばれる。無償のソフトウェアは、同種の有償のソフトウェアに比べて、その機能が一部制限されていたり、試用期間

や試用回数に制限を受けることが多い。無償のソフトウェアを試用することによりソフトウェアの価値を認めたユーザは、提供元のウェブサイトから有償のソフトウェアを購入してダウンロードしたり、販売店で有償のパッケージソフトウェアを購入したりしてバージョンアップを行う。

【0004】

一方、ソフトウェアはデジタルデータであり、複製が容易で、かつ複製による劣化も殆ど生じないという特徴を有するため、違法コピーや無断使用が大きな問題となっている。そこで、ソフトウェア（ソフトウェアのライセンス）を購入した正規ユーザとライセンスを得ていない違法ユーザとを、ユーザ認証等によって識別し、正規ユーザにのみソフトウェアを使用させるようにすることが従来より行われている。

【0005】

例えば、ソフトウェアをインストールする際に、ソフトウェアパッケージや記録媒体に印刷されたプロダクトIDを入力させて、正規購入品であるか否かを判定する技術は知られている（例えば、特許文献1）。

【0006】

また、ソフトウェアを使用するための鍵データをイントラネット上に設置されたライセンス管理サーバに要求し、ユーザ認証により正当なユーザと認められた場合には、ライセンス管理サーバから鍵データを取得し、この鍵データによってソフトウェアを起動させて使用するようにしたものも知られている（例えば、特許文献2、特許文献3）。

【0007】

【特許文献1】

特開2002-258963号公報 段落0003参照

【0008】

【特許文献2】

特開2002-6972号公報

【0009】

【特許文献3】

特開 2002-297254 公報

【0010】

【発明が解決しようとする課題】

プロダクトID（プロダクトキー）を入力することにより正規ユーザであるか否かを判別する従来技術は、単なる文字や記号からなるIDをインストール時に入力するだけの防御機構であり、容易に回避可能である。従って、この種の防御機構（著作権保護機構）しか備えないソフトウェアは、違法コピーや無断使用を事実上排除することができない。

【0011】

ライセンス管理サーバとの間でユーザ認証を行い、正常に認証された場合に鍵データをユーザコンピュータに送信して起動させる技術は、単にプロダクトIDを入力するだけの技術に比べて、防御力は向上している。しかし、ソフトウェアはユーザコンピュータ上で既に起動可能状態に置かれており、鍵データの取得待ちとなっている。従って、鍵データの入力待ち状態となっているソフトウェアを違法コピーし、別の方法で鍵データを取得してしまえば、防御機構をすり抜けて使用することができる。

【0012】

一方、近年では、コンピュータの処理能力増大及び通信ネットワークの高速化等に伴って、ユーザが希望する時に希望のソフトウェアを実行させる方法が提案されている。このようなソフトウェアのオンデマンド配信に適用可能な配信方法としては、ストリーミング方式とダウンロード方式とが知られている。

【0013】

ストリーミング方式では、ユーザコンピュータは、サーバからソフトウェアを受信しながら同時に再生を行う。そして、再生を終了して不要になったデータは直ちに破棄される。従って、ストリーミング方式は、ユーザの閲覧が終了した時点でデータが残らないため、特殊なソフトウェアを用いる等しない限り、違法にソフトウェアをコピーすることができない。しかし、ストリーミング方式では、ユーザが視聴を希望するたび毎に毎回ソフトウェアのデータを送信する必要があるため、広帯域で高速な通信ネットワークが整備されている場合でも、多数のユ

ーザが同時にストリーミング配信を希望すると、通信ネットワークのトラフィックが増大し、サーバの負担も大きくなる。

【0014】

これに対し、ダウンロード方式の場合は、ユーザの希望するソフトウェアをサーバからユーザコンピュータにダウンロードさせて蓄積し、ユーザコンピュータ上で実行させるため、データが通信ネットワークを流れる時間は少なく、多数のユーザからの配信要求に応えることができる。しかし、ダウンロード方式の場合は、ユーザコンピュータ内にソフトウェアが蓄積されたままになるため、ストリーミング方式よりも簡単に違法コピー等を行うことができる。

【0015】

そこで、本発明は、上記課題に鑑みてなされたもので、その目的は、ユーザコンピュータにソフトウェアを保存して実行させるダウンロード方式の場合に、違法コピーや無断使用を防止できるようにしたソフトウェア更新システム及びソフトウェアの実行制御プログラムを提供することにある。本発明の他の目的は、後述する実施の形態の説明から明らかになるであろう。

【0016】

【課題を解決するための手段】

本発明に係るソフトウェア更新システムは、ユーザコンピュータにインストールされた第1のソフトウェアを第2のソフトウェアに更新させるものであって、後述の配信手段及び認証手段を備え、かつ、特徴的な動作を行う実行制御プログラムを採用する。

【0017】

配信手段は、エンコードされた第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行制御プログラムをユーザコンピュータに通信ネットワークを介して配信するものである。認証手段は、ユーザコンピュータにインストールされた実行制御プログラムからの要求によってユーザ認証を行い、正当なユーザであると確認した場合には、第2のソフトウェアをデコードして起動させるために必要な所定の情報を通信ネットワークを介して実行制御プログラムに送信するものである。そして、第2のソフトウェアは実行制御プログラムから渡さ

れる起動情報のみで起動可能に構成されており、実行制御プログラムは、(1) 認証手段から受信した所定の情報に基づいてエンコードされた第2のソフトウェアをデコードして第1のソフトウェアに置き換え、(2) 所定の情報に基づいて起動情報を生成することにより、第2のソフトウェアを起動させ、(3) 第2のソフトウェアの実行が終了された場合には、第2のソフトウェアを無力化させるように構成されている。

【0018】

第1のソフトウェアと第2のソフトウェアとは、同一種類のソフトウェアであって、バージョンの異なるものである。第1のソフトウェアを旧版ソフトウェア、第2のソフトウェアを新版ソフトウェアと呼ぶこともできる。第1、第2のソフトウェアとしては、例えば、ゲーム、映画、娯楽番組、教養番組、教育番組、文書作成、図形作成、画像編集等の各種アプリケーションソフトウェアを採用することができる。第1のソフトウェアと第2のソフトウェアとは、例えば、使用言語、実行可能環境(対応OS等)、機能制限の有無等で相違する。ユーザコンピュータとしては、例えば、ワークステーション、パーソナルコンピュータ、携帯情報端末、携帯電話等を挙げることができる。

【0019】

最初に、ユーザコンピュータにインストールされている第1のソフトウェアは、後述の認証処理等を行わずに、ユーザが自由に使用することができる。第1のソフトウェアは、例えば、ソフトウェアベンダーのサイトからインターネット等の通信ネットワークを介して、あるいは、店頭販売のパッケージソフトウェアによって、ユーザコンピュータにインストールされている。

【0020】

次に、ユーザが、配信手段から第2のソフトウェアのダウンロードを希望すると、第2のソフトウェア及び第2のソフトウェアの実行を制御する実行制御プログラムが配信手段からユーザコンピュータに送信される。実行制御プログラムは、ユーザコンピュータ上で実行される。実行制御プログラムは、通信ネットワークを介して認証手段にユーザ認証を要求する。ユーザ認証の方法としては、例えば、ユーザID、パスワード、ユーザコンピュータに固有の情報(例えば、MAC

アドレス (Media Access Control address) 等) を予め登録されているデータと照合することにより行うことができる。なお、これに限らず、例えば、指紋や声紋等のユーザ固有の生体情報を用いて認証を行うようにしてもよい。

【0021】

認証手段が正当なユーザであると認証した場合は、認証手段からユーザコンピュータの実行制御プログラムに向けて、所定の情報が送信される。この所定の情報には、エンコードされた状態でユーザコンピュータに送信された第2のソフトウェアをデコードし、デコードされた第2のソフトウェアを起動させるために必要なデータが含まれている。

【0022】

ここで、第2のソフトウェアは、実行制御プログラムから渡される起動情報のみで起動可能に構成されている。即ち、実行制御プログラムは、第2のソフトウェアを起動させる専用の「ランチャーソフトウェア」として作用する。

【0023】

そして、実行制御プログラムは、以下の処理を行う。(1) まず、実行制御プログラムは、認証手段から受信した所定の情報に基づいて(所定の情報に含まれるデコードキーを利用して)、第2のソフトウェアをデコードする。デコードされた第2のソフトウェアは、第1のソフトウェアに置き換えられる。(2) 次に、実行制御プログラムは、認証手段から受信した所定の情報に基づいて(所定の情報に含まれる起動引数を利用して)、起動情報(起動引数とデコードされた第2のソフトウェアのレジストリパスからなる起動ステートメント)を生成し、この起動情報によって第2のソフトウェアを起動させる。これにより、ユーザは、ユーザコンピュータ上で第2のソフトウェアを使用することができる。(3) 実行制御プログラムは、第2のソフトウェアの起動後も、第2のソフトウェアの実行状態を監視しており、第2のソフトウェアの実行終了を検出すると、第2のソフトウェアを無力化させる。これにより、ユーザは、第2のソフトウェアを使用することができなくなる。

【0024】

ユーザが再度の使用を希望する場合、再び認証手段による認証を受けて所定の

情報を取得すればよい。あるいは、再びユーザコンピュータを配信手段にアクセスさせて、第2のソフトウェアを再度ダウンロードしてもよい。第2のソフトウェアの全体を再度ダウンロードする必要はなく、プログラム部分のみを再ダウンロードするように構成すれば、通信時間を短縮し、トラフィックを低減させることができる。なお、認証手段からユーザコンピュータに向けて送信される所定の情報は、暗号化されているのが好ましい。

【0025】

第2のソフトウェアの実行が終了すると、実行制御プログラムは、第2のソフトウェアを無力化させる。無力化とは、第2のソフトウェアを起動したり、実行したりできなくすることを意味する。無力化の方法としては、種々のものを採用することができる。例えば、デコードされた第2のソフトウェアの全体を削除することにより無力化することができる。また、デコードされた第2のソフトウェアの一部を削除することによっても無力化することができる。なお、一部のみを削除する場合は、その削除した部分及び起動引数を認証手段から受信することにより、第2のソフトウェアを再起動させることができる。あるいは、第2のソフトウェアがプログラムと付随データ群とを含んでなる場合、プログラムのみを削除することでも第2のソフトウェアを無力化させることができる。なお、デコード前のエンコードデータを保存しておくことにより、認証手段から所定の情報を再度受信するだけで第2のソフトウェアを再び使用することができる。付随データ群とは、プログラムの実行に際して利用されるプログラム以外のデータ群を意味し、例えば、画像データ、音声データ、楽曲データ、テキストデータ等を挙げることができる。

【0026】

好適な実施形態では、実行制御プログラムは、複数種類の第2のソフトウェアに対応可能に構成されており、認証手段が実行制御プログラムに送信する所定の情報には、起動させる第2のソフトウェアの格納先アドレス情報と起動引数と第2のソフトウェアをデコードするためのデコードキー情報とが含まれる。

【0027】

通信ネットワークを介したリアルタイムのオンライン認証と第2のソフトウェ

アの起動及び終了を制御する実行制御プログラムは、第2のソフトウェアとは別体に生成されている。従って、1種類の実行制御プログラムを用意するだけで、多種類の第2のソフトウェアに対応することができる。

【0028】

好適な実施形態では、実行制御プログラムは、ユーザコンピュータに固有のマシン情報と暗号化キー情報とを含む認証用情報を認証手段に送信し、認証手段は、少なくともマシン情報に基づいてユーザ認証を行い、正当なユーザであると確認した場合には、所定の情報を暗号化キー情報で暗号化して通信ネットワークを介して実行制御プログラムに送信するものであり、かつ、認証手段には、マシン情報を複数個登録可能に構成されている。

【0029】

ユーザコンピュータに固有のマシン情報としては、例えば、MACアドレス等を挙げることができる。これに加えて、ユーザコンピュータの構成情報（例えば、搭載メモリ量、CPUスペック、サウンドチップやグラフィックアクセラレータの製品名等）を採用してもよい。認証手段には、複数個のマシン情報を登録させることができる。これにより、第2のソフトウェアのライセンスを正当に購入したユーザは、例えば、自宅のパーソナルコンピュータと職場のパーソナルコンピュータ等のように、複数台のユーザコンピュータを用いて、同一の第2のソフトウェアを利用することができる。

【0030】

好適な実施形態では、認証手段は、正当なユーザであると確認した場合には、該ユーザが起動可能な第2のソフトウェアの一覧データをユーザコンピュータに送信し、一覧データから選択された第2のソフトウェアに関する所定の情報を通信ネットワークを介して実行制御プログラムに送信する。

【0031】

ユーザが複数種類の第2のソフトウェアのライセンスを正式に購入済の場合もあるが、認証手段は、ユーザ認証後に、そのユーザが利用可能な第2のソフトウェアの名称等を列挙した一覧データをユーザコンピュータに送信する。ユーザは、起動可能な（利用可能な）一覧メニューから起動を望む第2のソフトウェアを

選択する。これにより、認証手段は、選択された第2のソフトウェアをデコードし起動するための所定の情報を生成し、実行制御プログラムに送信する。

【0032】

好適な実施形態では、実行制御プログラムは、ユーザコンピュータに固有のマシン情報を取得する機能と、暗号化キー情報を生成する機能と、認証手段にユーザ認証を要求し、少なくともマシン情報及び暗号化キー情報を認証手段に送信する機能と、認証手段から受信した起動可能な第2のソフトウェアの一覧データからいずれか1つの第2のソフトウェアをユーザに選択させ、選択された第2のソフトウェアを認証手段に通知する機能と、選択された第2のソフトウェアのユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを少なくとも暗号化キー情報により暗号化してなる所定の情報を受信する機能と、暗号化された所定の情報を少なくとも暗号化キー情報により解読する機能と、解読されたデコードキー情報によりユーザコンピュータ内の第2のソフトウェアをデコードさせる機能と、解読された起動引数及び格納先アドレス情報に基づいて、起動情報を生成する機能と、生成された起動情報によってデコードされた第2のソフトウェアを起動させる機能と、起動された第2のソフトウェアの実行状態を監視し、該第2のソフトウェアの実行が終了した場合は、第2のソフトウェアを無力化させる機能と、をユーザコンピュータ上に実現させる。

【0033】

また、好適な実施形態では、第2のソフトウェアは、プログラムと付随データ群とを含んでなり、プログラム又は付随データ群の少なくともいずれか一方を更新させるようになっている。

【0034】

ここで、ユーザコンピュータにインストールされている第1のソフトウェアは、第2のソフトウェアに置換されるまでは、認証手段による認証を受けることなく実行可能である。

【0035】

また、好適な実施形態では、実行制御プログラムは、第2のソフトウェアとは別に強制終了させることができないプログラムとして構成されている。

【0036】

即ち、例えば、稼働中のタスクを管理するプログラム等を用いて、実行制御プログラムのみを強制終了させることができないように構成されている。実行制御プログラムによる監視を停止させて、第2のソフトウェアのみをコピー等できないようにするためである。より具体的には、ハードウェアを指定しないデバイスドライバとして実行制御プログラムを生成すれば（ハードウェアを指定しないので、厳密にはデバイスドライバではないが）、アプリケーションプログラムよりもOS側に近いプログラムあるいはOSの一部を構成するプログラムとして構成されるため、通常のアプリケーションプログラムのように強制的に終了させることが困難となる。強制終了させにくいプログラムとしては、ドライバプログラム他にBIOS (Basic Input/Output System) も知られている。しかし、BIOSは、基本的に、ハードウェアとの間で直接データを送受信するだけの機能しか持たないため、暗号化されたデータを復号化したり、第2のソフトウェアの実行を監視したりする等の高度な制御を行うことができない。このように、実行制御プログラムを、例えば、デバイスドライバのように、OSとアプリケーションプログラム（第2のソフトウェア）との間に位置する中間プログラムとして構成することにより、高度な処理を行わせつつ、悪用を防止することができる。

【0037】

好適な実施形態では、配信手段と認証手段とは、それぞれ別体のコンピュータ上に実現されている。

【0038】

例えば、第2のソフトウェア及び実行制御プログラムを配信する配信手段は、各ソフトウェア会社毎にそれぞれ設置し、第2のソフトウェアの起動時認証を行う認証手段は、各国、各地域、各ソフトウェア会社の団体毎に設置することができる。

【0039】

本発明は、プログラムの発明としても把握することができる。

【0040】

即ち、ユーザコンピュータにインストールされた第1のソフトウェアを第2の

ソフトウェアに更新し、この第2のソフトウェアの実行を制御する実行制御プログラムであって、外部の認証手段と通信ネットワークを介して通信し、ユーザ認証を求める第1の機能と、認証手段から受信した所定の情報に基づいて、第2のソフトウェアを起動させるための起動情報を生成する第2の機能と、認証手段から受信した所定の情報に基づいて、第2のソフトウェアをデコードさせる第3の機能と、ユーザコンピュータに既にインストールされている更新前のソフトウェアをデコードされた第2のソフトウェアに置き換える第4の機能と、生成された起動情報によって第2のソフトウェアを起動させる第5の機能と、第2のソフトウェアの実行状態を監視し、第2のソフトウェアの実行が終了した場合は、第2のソフトウェアを無力化させる第6の機能と、をユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

【0041】

また、本発明は、ソフトウェアの更新方法としても把握できる。

【0042】

即ち、ユーザコンピュータにインストールされている自由に使用可能な第1のソフトウェアを第2のソフトウェアに更新可能である旨をユーザに通知させるステップと、第2のソフトウェアを配信する配信用コンピュータにユーザコンピュータを通信ネットワークを介して接続させ、第2のソフトウェアへの更新を要求させるステップと、配信用コンピュータからユーザコンピュータにエンコードされた第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行制御プログラムを通信ネットワークを介して送信させるステップと、ユーザコンピュータ上で起動した実行制御プログラムにより、ユーザコンピュータと認証用コンピュータとを通信ネットワークを介して接続させ、認証用コンピュータにユーザ認証を要求させるステップと、ユーザ認証により正当なユーザであると認められた場合に認証用コンピュータからユーザコンピュータに送信される所定の情報に基づいて、第2のソフトウェアをデコードするステップと、認証用コンピュータから受信した所定の情報に基づいて、第2のソフトウェアを起動させるための起動情報を生成させるステップと、生成された起動情報によって第2のソフトウェアを起動させるステップと、起動された第2のソフトウェアの実行を監視し

、第2のソフトウェアの実行が終了した場合は、第2のソフトウェアを無効化させるステップと、を含んでなるソフトウェアの更新方法。

【0043】

【発明の実施の形態】

以下、本発明の実施形態を図1～図 を参照しつつ詳細に説明する。

【0044】

まず、図1は、本発明に係るソフトウェア更新システムの全体概要を示す説明図である。本実施形態では、ゲームプログラムをオンラインで更新させるシステムを例に挙げて説明する。

【0045】

配信用コンピュータ10は、新版のゲームプログラム40及び実行制御プログラム50を、インターネット等の通信ネットワークを介して、各ユーザのコンピュータ30に配信するためのものである。配信用コンピュータ10は、各ソフトウェア会社（ベンダー）毎にそれぞれ設置されるサーバとして構成することができる。

【0046】

まず、配信用コンピュータ10は、ゲームプログラムデータベース12に登録された新版プログラムについて、事前に、認証用コンピュータ20に登録を行う（S1）。例えば、新版ゲームプログラムの名称、種類、販売価格、データサイズ、バージョン情報等のデータが、配信用コンピュータ10から認証用コンピュータ20に登録される。もっとも、配信用コンピュータ10と認証用コンピュータとが一体的に構成されている場合は、このような通知は必要ない。

【0047】

配信用コンピュータ10の配信制御部11は、ユーザコンピュータ30からプログラムの更新要求を受けると、ユーザの希望するゲームプログラム40をゲームプログラムデータベース12から読み出して、ユーザコンピュータ30に配信するようになっている（S2）。ここで、新版のゲームプログラム40は、単独でユーザコンピュータ30に配信されるのではなく、ゲームプログラム40の起動や削除等を管理する実行制御プログラム50と共にユーザコンピュータ30に

配信される点に留意すべきである。

【0048】

認証用コンピュータ20は、例えば、複数のソフトウェア会社が所属する団体や機関毎にそれぞれ設置されるサーバとして構成することができる。また、これに限らず、各ソフトウェア会社毎に認証用コンピュータ20をそれぞれ設置してもよい。認証用コンピュータ20は、認証部21と、課金処理部22と、起動情報送信部23と、ユーザ情報データベース24と、ゲーム情報データベース25とを備えている。

【0049】

認証部21は、ユーザコンピュータ30の実行制御プログラム50から送信される所定の認証用データに基づいて、ユーザ認証を行うものである。詳細は後述するが、認証用データには、例えば、ユーザ識別情報（ユーザID）、パスワード（PW）、MACアドレス（Media Access Control address）が含まれる。

【0050】

課金処理部22は、新版ゲームプログラム40の使用許諾に際して、ユーザに課金するものである。課金方法には、種々のものを採用できる。例えば、ゲームプログラムの代金を一括でユーザに支払わせたり（売り切り）、又は、ユーザがゲームプログラムを使用する毎に課金してもよい。あるいは、所定期間や所定回数毎に課金するようにしてもよい。なお、支払方法も、例えば、クレジット決済、電子マネー決済等のように種々のものを採用できる。

【0051】

起動情報送信部23は、ユーザコンピュータ30の記憶装置（例えば、ハードディスク等）に格納された新版のゲームプログラム40をデコードし、起動させるために必要な起動情報をユーザコンピュータ30の実行制御プログラム50に向けて送信するものである。

【0052】

ユーザが、実行制御プログラム50を介して認証用コンピュータ20の認証部21と認証を行い、ゲームプログラム40の購入代金（使用権の代金）を支払い済みの正当なユーザであると認証された場合は（S3）、起動情報送信部23か

ら起動情報が実行制御プログラム 50 に送信される (S 4)。ゲームプログラム 40 の代金を未払いのユーザが認証用コンピュータ 20 にアクセスした場合は、課金処理部 22 を介して課金処理が行われた後、起動情報が実行制御プログラム 50 に向けて送信される。

【0053】

さて、ユーザコンピュータ 30 の構成に目を転じると、ユーザコンピュータ 30 は、例えば、パーソナルコンピュータ、ワークステーション、携帯情報端末、携帯電話等のコンピュータとして構成されている。ユーザコンピュータ 30 は、演算処理装置 (CPU)、主記憶、補助記憶、外部入出力回路等のコンピュータ資源を備えており、これらの各資源は適宜ゲームプログラム 40 及び実行制御プログラム 50 によって使用される。

【0054】

配信用コンピュータ 10 からユーザコンピュータ 30 に送信された新版のゲームプログラム 40 及び実行制御プログラム 50 は、後述のように、付属するインストーラによってユーザコンピュータ 30 にインストールされる。そして、実行制御プログラム 50 が認証用コンピュータ 20 との間でユーザ認証を行い、起動情報を入手すると、ゲームプログラム 40 が起動される (S 5)。なお、新版のゲームプログラム 40 をインストールするより前に、ユーザコンピュータ 30 に既にインストールされていた旧版のゲームプログラムは、新版のプログラムに置き換えられるため、以後使用することができなくなる。

【0055】

ユーザは、ユーザコンピュータ 30 を介して新版のゲームプログラム 40 を利用することができる。そして、ユーザがゲームを終えて、ゲームプログラム 40 を終了させると、実行制御プログラム 50 は、ゲームプログラム 40 を削除する等して無力化する (S 6)。ユーザがゲームプログラム 40 を再び利用する場合は、認証用コンピュータ 20 に再度アクセスしてユーザ認証を行い、起動情報を取得する。

【0056】

ここで、ユーザコンピュータ 30 の記憶装置内には、新版のゲームプログラム

40がデコード前の圧縮ファイルの状態で保存されているため、ゲームプログラム40を再使用する場合は、この圧縮ファイルをデコードするための情報（デコードキー）と起動させるための情報とを認証用コンピュータ20から取得するだけでよい。即ち、本実施形態では、ユーザコンピュータ30のローカルディスクに新版ゲームプログラム40を圧縮ファイルの状態で保存しておき、ゲームを行うたびに、認証用コンピュータ20との間でオンライン認証を行って、圧縮されたゲームプログラム40をデコードして起動させる。そして、ゲーム終了後には、デコードされたゲームプログラム40を削除して無力化させる。

【0057】

次に、図2は、認証用コンピュータ20が利用するユーザ情報データベース24及びゲーム情報データベース25の構造例を示す説明図である。なお、図2に示す各データベース24、25の内容は一例であって、図示する項目の全てを備える必要はない。

【0058】

図2（a）に示すユーザ情報データベース24は、例えば、ユーザIDと、パスワードと、複数のMACアドレス1～nと、購入済のゲームプログラムを特定するゲームID1～nと、その他の情報とをそれぞれ対応付けることにより構成されている。ここで、複数のMACアドレス1～nを登録可能としたのは、1人のユーザがそれぞれ異なる複数のユーザコンピュータ30を用いて、ゲームプログラム40を使用する場合も考慮したためである。従って、ユーザは、例えば、職場のコンピュータ、自宅のコンピュータ等の異なる情報処理端末を介して、ゲームプログラム40を利用できるようになっている。その他の情報としては、例えば、ユーザの氏名、年齢、住所、ゲームのプレイ回数、獲得したポイント数（例えば、ゲーム購入代金やプレイ回数等に応じてポイントを与えるような場合）等を挙げることができる。

【0059】

図2（b）に示すゲーム情報データベース25は、例えば、ゲームIDと、ゲーム名と、ゲーム情報（ゲームプログラムのレジストリパスを示す情報）と、圧縮されたゲームプログラム40を復号するためのデコードキーと、デコードされ

たゲームプログラム 40 を起動させるための起動引数と、その他の情報とをそれぞれ対応付けることにより構成されている。その他の情報としては、例えば、ゲームの種類（ロールプレイングゲーム、格闘ゲーム、成人指定の有無等）、データサイズ、著作権管理情報等を挙げることができる。

【0060】

図 2（c）に示すように、ゲーム情報、デコードキー及び起動引数は、暗号化されて HTML（Hyper Text Markup Language）データに埋め込まれ、ユーザコンピュータ 30 に送信されるようになっている。即ち、ユーザコンピュータ 30 側で生成された暗号化キー及び MAC アドレスによって、起動情報（ゲーム情報、デコードキー、起動引数）は暗号化され、例えば、HTML のヘッダ部に埋め込まれる。従って、認証用サーバ 20 は、ユーザコンピュータ 30 からの HTTP（Hyper Text Transport Protocol）リクエストに応じて、暗号化された起動情報を生成し、この暗号化された起動情報を含んだ HTTP レスポンスをユーザコンピュータ 30 に返すようになっている。

【0061】

次に、図 3 は、ゲームプログラム 40 及び実行制御プログラム 50 の概略構成を示す説明図である。

【0062】

図 3（a）に示すように、ゲームプログラム 40 は、プログラム本体 41 と、付随データ群 42 とを含んでいる。付随データ群 42 としては、例えば、動画像データ、静止画像データ、グラフィックスデータ、楽曲データ、音声データ、テキストデータ等を挙げることができる。

【0063】

新版のゲームプログラム 40 は、旧版のプログラムに比較して、プログラム 41 又は付随データ群 42 のいずれか又は双方が新しく作成されている。プログラム本体 41 及び付随データ群 42 の両方が旧版よりも新しい場合は、プログラム本体 41 及び付随データ群 42 の両方が新版に置き換えられる。付随データ群 42 のみが新しい場合及びプログラム本体 41 のみが新しい場合は、付随データ群 42 又はプログラム本体 41 のいずれかが新版に置き換えられる。

【0064】

図3 (b) に示すように、実行制御プログラム50は、ユーザコンピュータ30上で、暗号用情報生成部51と、認証要求部52と、ゲーム選択部53と、暗号解読部54と、起動部55と、デコード部56と、実行監視部57という各機能を実現させる。実行制御プログラム50は、デバイスを特定しないデバイスドライバとして構成されている。このため、実行制御プログラム50は、ゲームプログラム等のアプリケーションプログラムとは異なって、タスク管理プログラム等から終了させることができないようになっている。

【0065】

暗号情報生成部51は、例えば、ユーザコンピュータ30の内蔵タイマから取得した時刻情報に基づいて暗号化キーを生成するほか、ユーザコンピュータ30のMACアドレスを取得する。

【0066】

認証要求部52は、ユーザコンピュータ30に実装されているウェブブラウザの機能を内部的に呼び出して、認証用コンピュータ20にアクセスし、暗号化キー、MACアドレス、ユーザID及びパスワードを認証用コンピュータ20に送信してユーザ認証を求める。

【0067】

ゲーム選択部53は、ユーザ認証が終了して認証用コンピュータ20からユーザコンピュータ30に送信された一覧メニューから、ユーザが希望するゲームを選択させる。この一覧メニューは、ユーザが利用可能な（起動可能な）ゲームプログラムを一覧形式で表示させるものであり、ユーザ情報データベース24の購入済ゲームIDに基づいて生成することができる。

【0068】

暗号化情報生成部51によって生成された暗号化キー及びMACアドレスにより、ユーザの選択したゲームプログラム40を起動させるための起動情報は、暗号化されてユーザコンピュータ30に送信される。暗号解読部54は、暗号化キー及びMACアドレスに基づいて、暗号化された起動情報を解読する。

【0069】

デコード部 56 は、解読されたデコードキーによって、圧縮されたゲームプログラム 40 をデコードさせる。なお、圧縮ファイルはそのまま保存される。起動部 55 は、解読されたゲーム情報及び起動引数に基づいて、起動ステートメントを生成し、デコードされたゲームプログラム 40 を起動させる。起動ステートメントは、ゲームプログラムのレジストリパスと起動引数から構成される。

【0070】

ゲームプログラム 40 が起動されると、実行監視部 57 は、ゲームプログラム 40 の実行状態を監視し、ゲームプログラム 40 が終了すると、デコードされたプログラム本体 41 を削除する。なお、デコードした付随データ群も一緒に削除してもよい。また、削除する場合は、プログラム又はデータの全部を削除してもよいし、一部を削除してもよい。

【0071】

次に、図 4 は、本システムによってゲームプログラムを最新版に更新する様子を模式的に示す説明図である。

【0072】

まず、図 4 (a) に示すように、ユーザコンピュータ 30 には、旧版のゲームプログラムが既にインストールされている。なお、図中では、バージョンアップ前の旧版のゲームプログラムを「初期プログラム」と、バージョンアップする新版のゲームプログラムを「更新版プログラム」とそれぞれ表示する。

【0073】

ユーザは、例えば、CD-ROM、DVD-ROM、メモリ等の記録媒体に固定された旧版のゲームプログラム 40A をユーザコンピュータ 30 にインストールして利用する (S11)。あるいは、インターネット等の通信ネットワークを介して旧版のゲームプログラム 40A を取得することもできる。この旧版のゲームプログラム 40A は、認証用コンピュータ 20 とのオンライン認証を受けることなく使用可能である。但し、本更新システムによっていったん更新された後は、更新版プログラムが旧式になった場合でも、オンライン認証を受けなければ利用することはできない。

【0074】

旧版のゲームプログラム 40A を利用するユーザには、新版ゲームプログラム 40 へアップデート可能である旨が通知される。この通知は、種々の方法で行うことができる。

【0075】

第1の方法は、例えば、旧版のゲームプログラム 40A が、積極的又は消極的に、ユーザに新版のゲームプログラム 40 へ更新可能であることを通知し、併せて、配信用コンピュータ 10 の URL (Uniform Resource Locator) を表示する方法である。積極的な通知としては、例えば、ゲーム開始時や終了時等に更新可能である旨及び配信用コンピュータ 10 の URL を画面に表示させることが考えられる。消極的な通知としては、例えば、旧版のゲームプログラム 40A のヘルプメニューの中に、更新可能である旨及び配信用コンピュータ 10 の URL を表示させることが考えられる。いずれの場合も、URL をクリックするだけで、ウェブブラウザ 31 を起動させ、自動的にユーザコンピュータ 30 を配信用コンピュータ 10 にアクセスさせるように構成すると、ユーザの使い勝手が良い。

【0076】

第2の方法は、電子的な媒体を介して積極的又は消極的に、新版のゲームプログラム 40 へ更新可能である旨及び配信用コンピュータ 10 の URL を、ユーザに通知する方法である。積極的な通知としては、例えば、ユーザ宛の電子メールを挙げることができる。消極的な通知としては、例えば、ウェブ上のサイト（例えば、配信用コンピュータ 10 等）で、新版のゲームプログラム 40 を広告宣伝することが考えられる。

【0077】

第3の方法としては、その他、ゲーム雑誌やコンピュータ雑誌等の紙媒体上での広告宣伝、ネットワーク上に形成されたゲームプログラム同好会のようなコミュニティへの広告宣伝等を用いることができる。

【0078】

以上のようにして、ユーザに対し、新版ゲームプログラム 40 の存在を通知させることができる。図4(b)に示すように、更新を希望するユーザは、ウェブブラウザ 31 を介して配信用コンピュータ 10 にアクセスし、新版ゲームプログ

ラム 40 への更新を要求する (S12)。

【0079】

図 4 (c) に示すように、配信用コンピュータ 10 は、ユーザの希望する新版のゲームプログラム 40 (付随データ群も含まれる) を、通信ネットワークを介して、ユーザコンピュータ 30 に向けて送信する (S13)。また、新版のゲームプログラム 40 と一緒に実行制御プログラム 50 もセットにしてユーザコンピュータ 30 に送信される (S13)。新版のゲームプログラム 40 及び実行制御プログラム 50 は、ユーザコンピュータ 30 の記憶装置に保存される。

【0080】

新版のゲームプログラム 40 及び実行制御プログラム 50 には、専用のインストーラが付属している。インストーラにより、新版のゲームプログラム 40 及び実行制御プログラム 50 がユーザコンピュータ 30 にインストールされる。実行制御プログラムが起動すると、図 4 (d) に示すように、実行制御プログラム 50 は、ウェブブラウザの機能呼び出して、認証用コンピュータ 20 にアクセスし、認証用コンピュータ 20 との間で、ユーザ認証及び購入処理 (課金処理) を行う (S14)。ユーザ認証や課金処理を終えた後で、認証用コンピュータ 20 は、ユーザコンピュータ 30 の実行制御プログラム 50 に向けて、暗号化された起動情報を送信する (S15)。

【0081】

実行制御プログラム 50 は、暗号化された起動情報を解読して、デコードキーや起動引数等を取り出す。そして、実行制御プログラム 50 は、ゲームプログラム 40 をデコードして起動させる。これにより、ユーザは、新版のゲームプログラム 40 を利用することができる。ゲームプログラム 40 の実行状態は、実行制御プログラム 50 により監視される。

【0082】

図 4 (e) に示すように、ユーザがゲームプレイを終了し、ゲームプログラム 40 が終了すると、実行制御プログラム 50 は、新版のゲームプログラム 40 を削除することにより無力化させる (S16)。

【0083】

ここで、留意すべき点は、デコードされて実行可能な状態（起動ステートメントの入力により起動可能な状態）に置かれている新版のゲームプログラム 40 のみを削除し、配信用コンピュータ 10 から取得したデコード前の圧縮ファイルは、ユーザコンピュータ 30 の記憶装置内に保存しておく点にある。

【0084】

これにより、ユーザがゲームプログラム 40 の再プレイを希望する場合は、認証用コンピュータ 20 にアクセスしてオンラインによるユーザ認証を受け、認証用コンピュータ 20 から起動情報を改めて取得するだけで足りる（S17）。圧縮状態のゲームプログラム 40 を配信用コンピュータ 10 から改めて取得する必要がないため、ダウンロードの手間がかからず、また通信ネットワークへの負担を軽減することができる。

【0085】

このように、ゲームプログラム 40 を再度プレイする場合は、ゲームプログラム 40 の起動情報のみを再取得する方法が便利であるが、本発明はこれに限らず、デコード前の圧縮されたプログラムを配信用コンピュータ 10 から再度取得するようにしてもよい。また、デコードされたプログラム本体 41 のみを削除し、付随データ群 41 をそのまま残してもよい。

【0086】

次に、図 5 及び図 6 に基づいて、本システムの処理の詳細を説明する。図に示すフローチャートは、処理の大まかな流れを示すものであり、実際のプログラムとは相違する。

【0087】

図 5 は、ユーザコンピュータ 30 の記憶装置に格納された新版のゲームプログラム 40 及び実行制御プログラム 50 をインストール等する処理を示す。

【0088】

ゲームプログラム 40 及び実行制御プログラム 50 は圧縮ファイルの状態でユーザコンピュータ 30 に保存される。例えば、ユーザが、圧縮ファイルをマウスポインタで選択してダブルクリックする等のように、起動イベントを発生させると、インストーラが起動する（S21）。

【0089】

インストーラは、ユーザコンピュータ30に更新すべき旧版のゲームプログラム40Aがインストール済であるか否かを判定する(S22)。旧版のゲームプログラム40Aがインストールされていない場合は、例えば、「旧版のゲームがインストールされていません。処理を終了します。」等のような警告メッセージを画面に表示させて終了する(S23)。

【0090】

旧版のゲームプログラム40Aがユーザコンピュータ30にインストールされている場合は(S22:YES)、新版のゲームプログラム40及び実行制御プログラム50を初めてインストールするの否かを判定する(S24)。新版ゲームプログラム40及び実行制御プログラム50が過去にインストールされている場合は、既にユーザ登録及び課金処理が完了しているものとみなすことができる。従って、S24は、結果的に、既にユーザ登録及び課金処理が完了しているか否かを判定することになる。

【0091】

初めてのインストールである場合は、ウェブブラウザ31の機能呼び出して認証用コンピュータ20に接続し、ユーザに、ユーザ登録及び課金処理を行わせる(S25, S26)。

【0092】

次に、インストーラは、実行制御プログラム50のレジストリを判定し、実行制御プログラム50が未だインストールされていない場合は、実行制御プログラム50をインストールする(S27)。インストーラは、旧版のゲームプログラム40Aを新版のゲームプログラム40に置き換えて更新すべく、旧版のプログラム本体41及び付随データ群42を新版のプログラム本体41及び付随データ群42に書き換える(S28, S29)。そして、インストーラは、実行制御プログラム50を起動させて処理を終了する(S30)。

【0093】

図6は、実行制御プログラム50による実行制御処理及び認証用コンピュータ20の処理等を示すフローチャートである。

【0094】

起動された実行制御プログラム50は、ユーザコンピュータ30に固有のマシン情報、具体的には、MACアドレスを取得する(S41)。また、ユーザコンピュータ30の内蔵タイマから現在時刻の情報を取得し、この時刻情報に基づいて暗号化キーを生成する(S42)。

【0095】

次に、実行制御プログラム50は、ウェブブラウザ31の機能呼び出し(S43)、通信ネットワークを介して認証用コンピュータ10に接続し、認証用コンピュータ20にログイン認証を要求する(S44)。実行制御プログラム50は、ユーザID、パスワード、MACアドレス及び暗号化キーを認証用コンピュータ20に送信する(S44)。認証用コンピュータ20は、ユーザ情報データベース24を参照し、正当なユーザであるか否かを判断する(S61)。

【0096】

正当なユーザであると認められた場合、認証用コンピュータ20は、ユーザが利用可能なゲームプログラムの一覧データを作成し、ユーザコンピュータ30に送信する(S62)。ユーザが利用することができるゲームプログラムとしては、典型的には、そのユーザが購入しているゲームプログラムを挙げることができるが、これに限らず、例えば、ソフトウェア会社が無償で提供しているゲームプログラム等を含めることもできる。

【0097】

実行制御プログラム50は、利用可能なゲームプログラムの一覧データを認証用コンピュータ20から受信すると、ユーザコンピュータ30のモニタディスプレイにゲームの一覧を表示させる(S45)。この一覧メニューに基づいて、ユーザは、プレイを希望するゲームを選択する(S46)。

【0098】

認証用コンピュータ20は、ゲーム情報データベース25を参照して、ユーザが選択したゲームプログラムを起動させるために必要な起動情報を生成し、この起動情報を、S61で取得した暗号化キー及びMACアドレスによって暗号化する(S63)。認証用コンピュータ20は、暗号化された起動情報をユーザコンピ

ュータ 30 の実行制御プログラム 50 に送信する (S64)。

【0099】

実行制御プログラム 50 は、暗号化された起動情報を認証用コンピュータ 20 から受信すると (S47)、この暗号化された起動情報を暗号化キー及び MAC アドレスによって解読する (S48)。

【0100】

次に、実行制御プログラム 50 は、新版のゲームプログラム 40 のレジストリ情報を取得し (S49)、レジストリパスと起動引数とによって起動ステートメントを生成する (S50)。

【0101】

また、実行制御プログラム 50 は、起動情報から取り出したデコードキーによって、圧縮された新版のゲームプログラム 40 をデコードし、所定のドライブの所定のディレクトリに展開させる (S51)。これにより、ゲームプログラム 40 はデコードされて起動待ちの状態になる。

【0102】

そして、実行制御プログラム 50 は、S50 で生成した起動ステートメントによって、デコードされた新版のゲームプログラム 40 を起動させる (S52, S70)。これにより、ユーザは、新版のゲームプログラム 40 で遊ぶことができる (S71)。

【0103】

実行制御プログラム 50 は、ゲームプログラム 40 の実行状態を監視しており (S53)、ユーザがゲームを終えてゲームプログラム 40 を終了させた場合には (S72)、デコードされたプログラム本体 41 を削除等することにより、ゲームプログラム 40 を無力化し、処理を終了する (S54)。

【0104】

なお、ユーザが再びゲームプログラム 40 で遊びたい場合は、再度認証用コンピュータ 20 にアクセスしてオンラインによる認証を受け、起動情報を取得すればよい。

【0105】

このように構成される本実施の形態によれば、ユーザコンピュータ 30 にプログラムを格納させるダウンロード式のソフトウェア配信の場合でも、使用権を購入していない違法な使用を阻止することができる。

【0106】

即ち、本実施形態において、ゲームプログラム 40 を起動させるには、使用する度毎に、実行制御プログラム 50 を介してオンラインによる認証を行い、認証用コンピュータ 20 から通信ネットワークを介して起動情報を取得する必要があるため、仮に、ゲームプログラム 40 のみを単体で違法にコピーしても、違法にコピーされたゲームプログラム 40 を単体で起動させることはできない。

【0107】

また、実行制御プログラム 50 はデバイスドライバのように OS 側に近いプログラムとして構成されており、アプリケーションプログラムのように通常の方法では終了させることができない。従って、実行制御プログラム 50 とゲームプログラム 40 とを切り離して、ゲームプログラム 40 のみを違法にコピーしたり持ち出したりすることができないようになっている。

【0108】

本発明は、種々のビジネスに活用することができるであろう。例えば、過去に違法にコピーされて流通している旧版ゲームプログラムを、新版ゲームプログラムに更新させることにより、違法使用のユーザに正式に使用権を取得させて、正当なユーザへ変えることができる。違法なユーザを新版のゲームプログラムに乗り換えさせるためには、そのユーザの母国語に対応した付随データ群（ゲームシナリオや楽曲等）を用意したり、追加のシナリオ等を新しく用意したりして、ユーザの更新意欲を刺激すればよい。

【0109】

なお、上述した本発明の実施の形態は、本発明の説明のための例示であり、本発明の範囲を実施形態にのみ限定する趣旨ではない。当業者は、本発明の要旨を逸脱することなしに、他の様々な態様で本発明を実施できる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態に係るソフトウェア更新システムの全体概要を示す説明図である。

【図 2】

データベース等の構造を示し、(a) はユーザ情報データベースを、(b) はゲーム情報データベースを、(c) は HTML ヘッダ内に暗号化された起動情報を埋め込んで送信する様子を、それぞれ示す。

【図 3】

プログラムの概略構造を示し、(a) はゲームプログラムを、(b) は実行制御プログラムの構造を、それぞれ示す。

【図 4】

ユーザコンピュータにインストールされた旧版のゲームプログラムを、新版のゲームプログラムに更新し、起動を制御する様子を示す説明図である。

【図 5】

ゲームプログラム及び実行制御プログラムをインストールするときの処理を示すフローチャートである。

【図 6】

実行制御プログラム及び認証用コンピュータとの間で行われるオンライン認証等を示すフローチャートである。

【符号の説明】

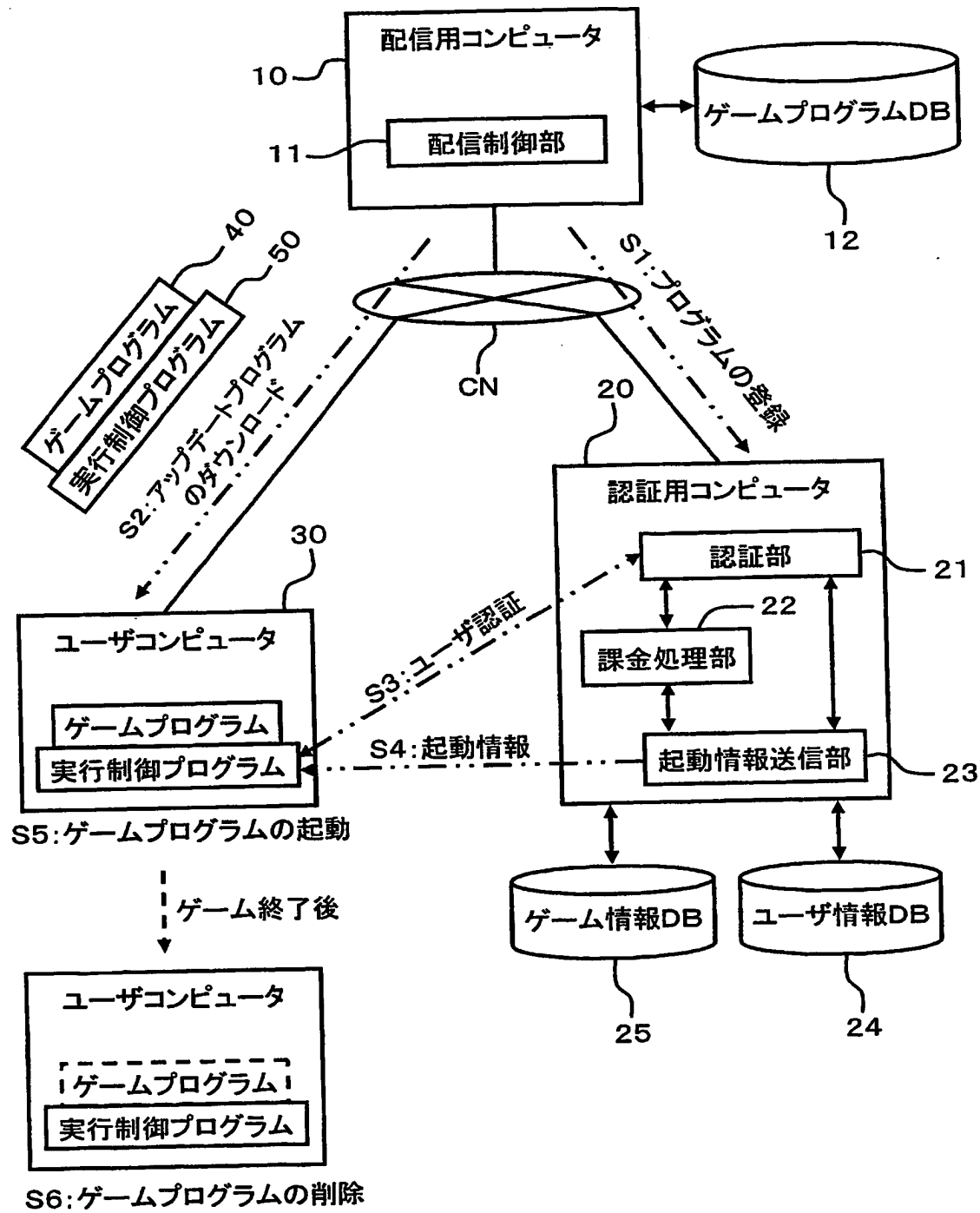
- 10 配信用コンピュータ
- 11 配信制御手段
- 12 ゲームプログラムデータベース
- 20 認証用コンピュータ
- 21 認証部
- 22 課金処理部
- 23 起動情報送信部
- 24 ユーザ情報データベース
- 25 ゲーム情報データベース
- 30 ユーザコンピュータ


- 3 1 ウェブブラウザ
- 4 0 新版のゲームプログラム
- 4 0 A 旧版のゲームプログラム
- 4 1 プログラム本体
- 4 2 付随データ群
- 5 0 実行制御プログラム
- 5 1 暗号用情報生成部
- 5 2 認証要求部
- 5 3 ゲーム選択部
- 5 4 暗号解読部
- 5 5 起動部
- 5 6 デコード部
- 5 7 実行監視部

【書類名】

凶面

【図 1】





【図 2】

(a) ユーザ情報データベースの構造

—24—

ユーザID	パスワード	MACアドレス1	...	MACアドレスn	購入済ゲームID1	...	購入済ゲームIDn	その他
-------	-------	----------	-----	----------	-----------	-----	-----------	-----

(b) ゲーム情報データベースの構造

—25—

ゲームID	ゲーム名	ゲーム情報	デコードキー	起動引数	その他
-------	------	-------	--------	------	-----

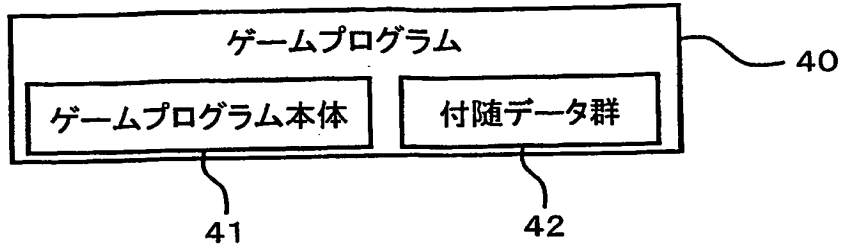
(c) 暗号化データの送信フォーマット

<HEAD>
<META>
<ST>
暗号化データ列
(ゲーム情報、デコードキー、起動引数)
<ED>
</META>
</HEAD>

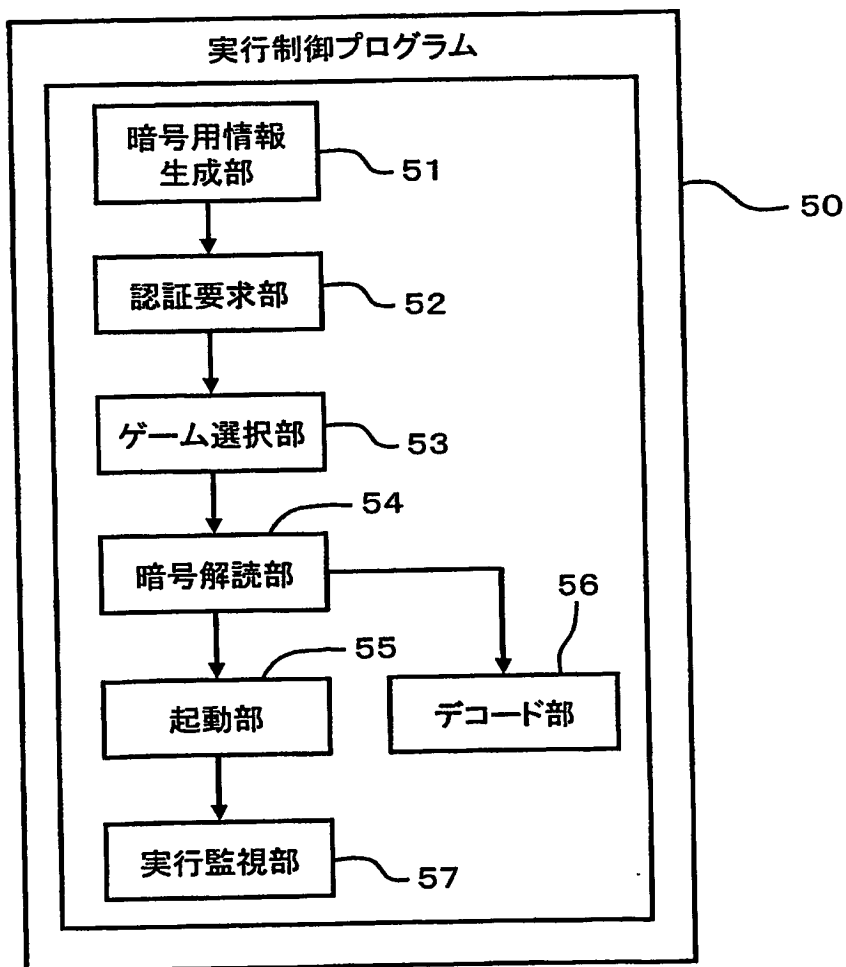
.
.
.

【図 3】

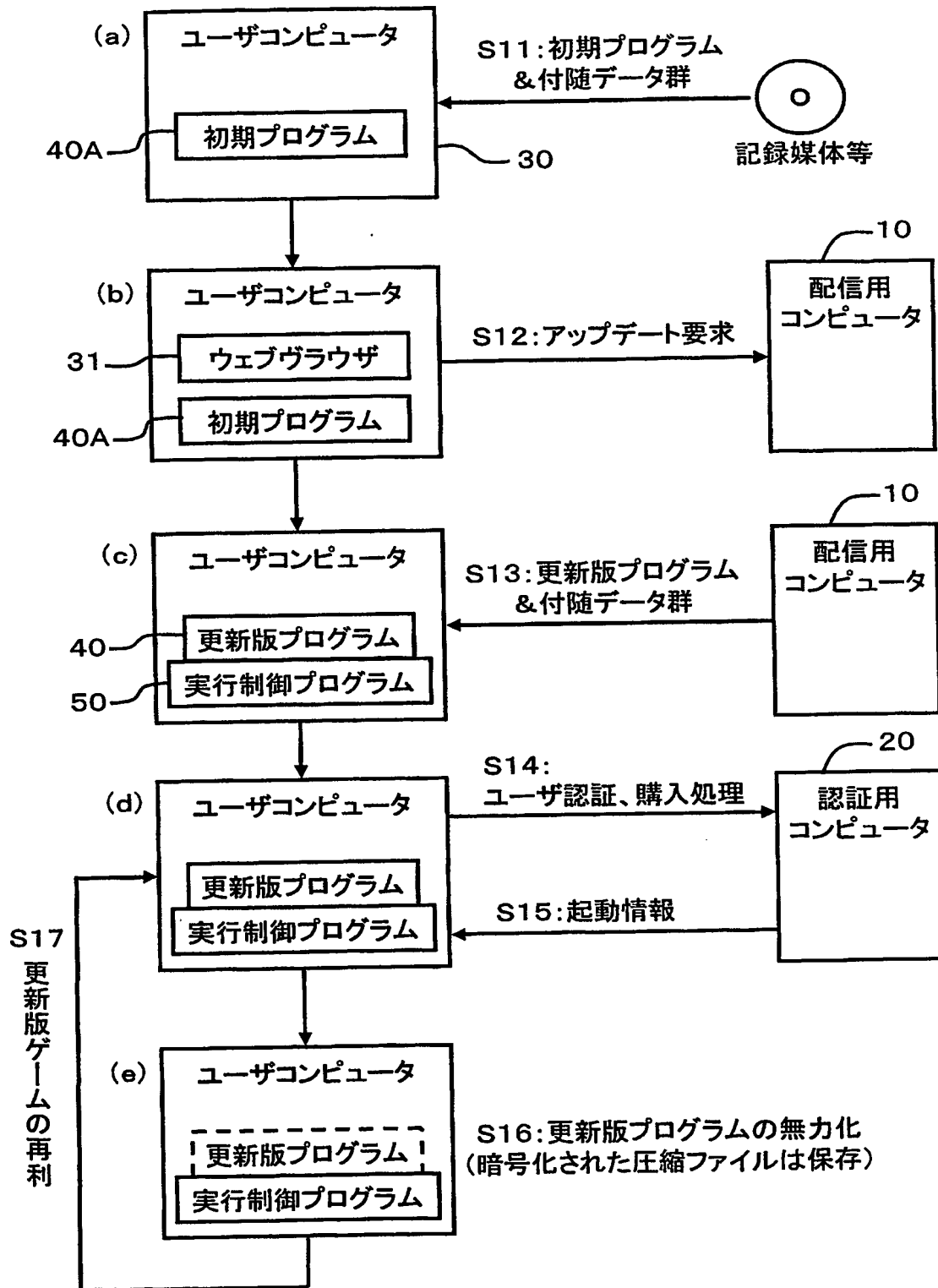
(a) ゲームプログラムの構造



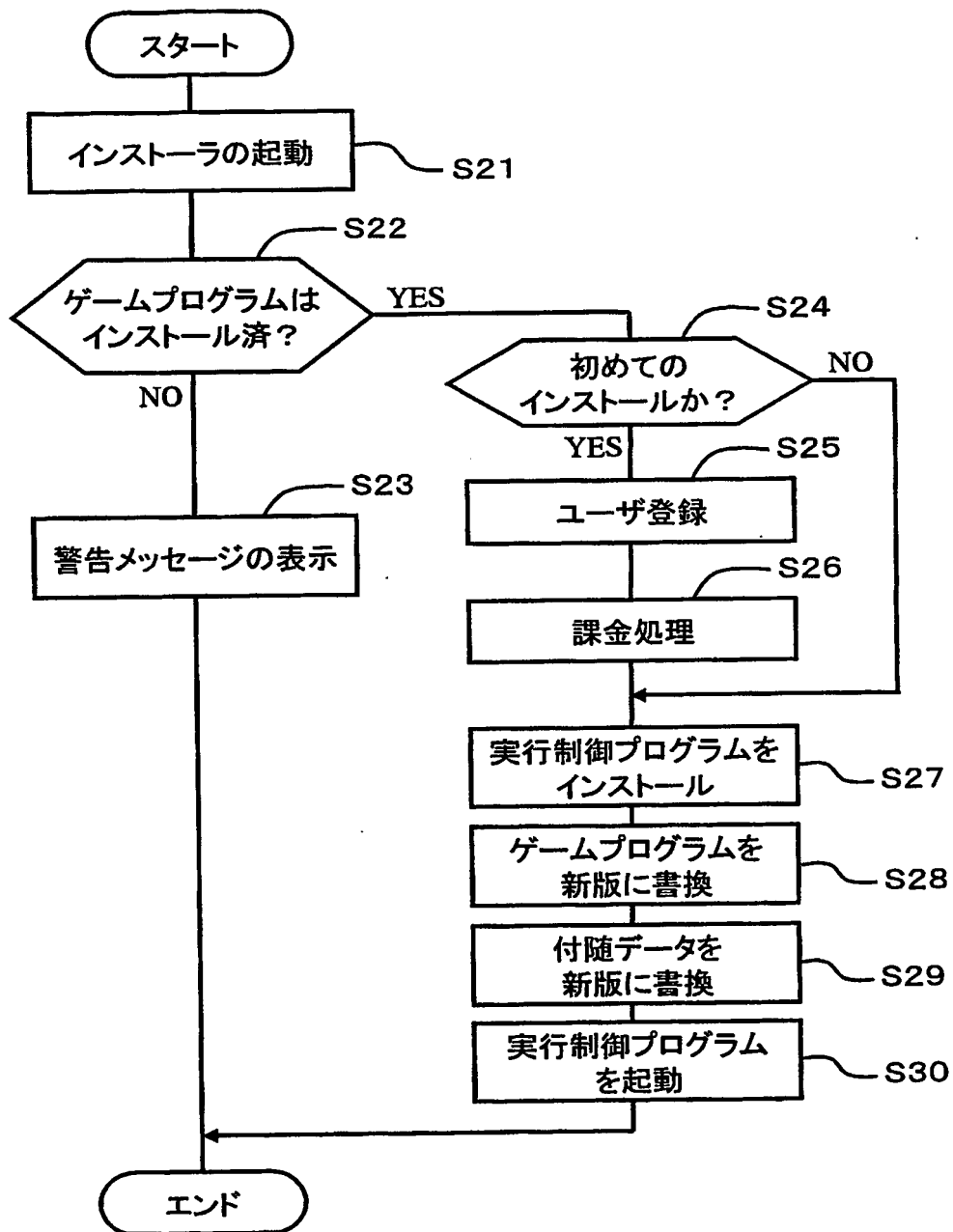
(b) 実行制御プログラムの構造



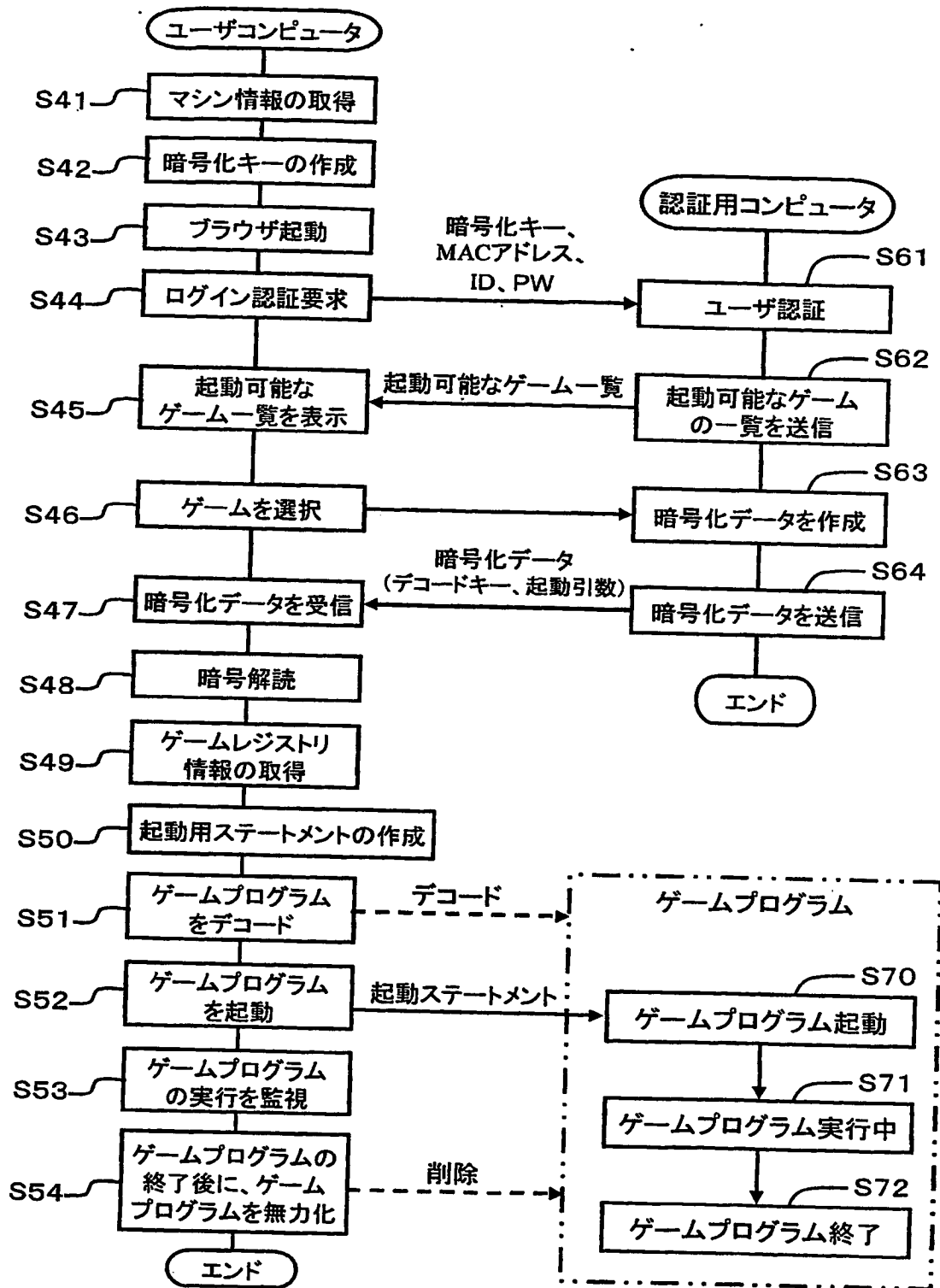
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 ユーザコンピュータに予めプログラムやデータを格納させて利用するダウンロード式のソフトウェア配信において、ゲームプログラム等のソフトウェアの違法な使用を未然に阻止する。

【解決手段】 ユーザは、配信用コンピュータ10から新版のゲームプログラム40（付随データ群も含む）及び実行制御プログラム50をダウンロードする（S2）。実行制御プログラム50は、認証用コンピュータ20とオンラインによる認証を行って、ゲームプログラム40を起動させるために必要な起動情報を取得する（S3, S4）。実行制御プログラム50は、起動情報に基づいてゲームプログラム40をデコードし、起動させる（S5）。ユーザがゲームを終えて、ゲームプログラム40を終了させると、実行制御プログラム50は、ゲームプログラム40の全部又は一部を削除することにより無力化する（S6）。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2002-359597
受付番号	50201877147
書類名	特許願
担当官	土井 恵子 4264
作成日	平成14年12月12日

<認定情報・付加情報>

【提出日】	平成14年12月11日
-------	-------------

次頁無

特願 2002-359597

ページ: 1/E

出願人履歴情報

識別番号

[500058589]

1. 変更年月日

2000年11月27日

[変更理由]

名称変更

住所

東京都港区芝浦2-17-13

氏名

インターレックス株式会社